PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 9/00, 9/62

A1

(11) International Publication Number: WO 98/25227

(43) International Publication Date: 11 June 1998 (11.06.98)

(21) International Application Number: PCT/CA97/00924

(22) International Filing Date: 2 December 1997 (02.12.97)

(30) Priority Data:
08/760,228 4 December 1996 (04.12.96) US

(71) Applicant *(for all designated States except US)*: DEW ENGINEERING AND DEVELOPMENT LIMITED [-/CA]; 3429 Hawthorne Avenue, Ottawa, Ontario K1G 4G2 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HAMID, Lawrence [CA/CA]; 124 Pretoria Avenue, Ottawa, Ontario K1S 1W9 (CA). FREEDMAN, Gordon [CA/CA]; 41 Elvaston Avenue, Nepean, Ontario K2G 3Y1 (CA).

(74) Agent: FREEDMAN, Gordon; Neil Teitelbaum & Associates, 834 Colonel By Drive, Ottawa, Ontario K1S 5C4 (CA).

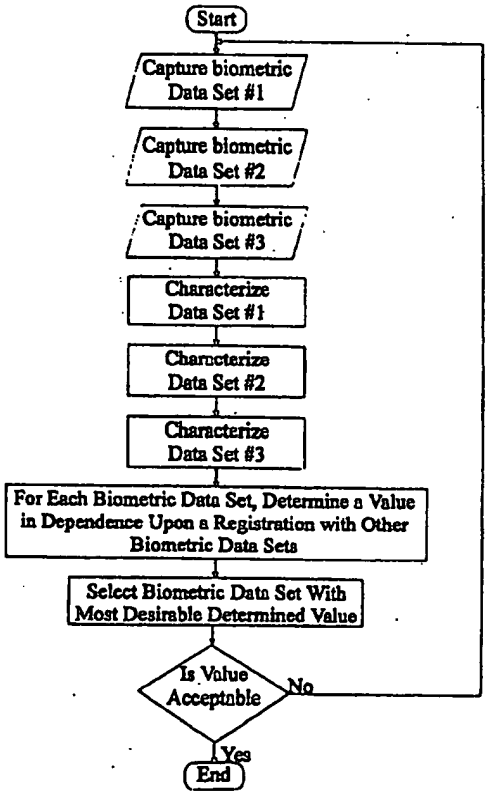
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: BIOMETRIC SECURITY ENCRYPTION SYSTEM

(57) Abstract

A method of registering biometric data for use in determining a template for user verification is disclosed wherein a number of instances on input biometric data are accepted from each user during a registration process. Each input biometric data is selected to act as a template and other biometric data are registered against the template. Registrations are evaluated and scores are accorded to each template. As long as a biometric template registers other biometric templates as matching and does so with a certainty above a predetermined threshold (resulting in a score within a predetermined range), the biometric data with the most desirable score is selected for determining the template for the user.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Biometric Security Encryption System

Field of the Invention

This invention relates generally to identification of individuals and more particularly relates to a method of selecting a biometric template for identification of individuals.

Background of the Invention

Computer security is fast becoming an important issue. With the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. A common method of providing security is using passwords. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

Preset codes are often forgotten as users have no reliable method of remembering them. Writing down the codes and storing them in close proximity to the access control device (i.e. The combination lock) results in a secure access control system with a very insecure code. Alternatively, the nuisance of trying several code variations renders the access control system more of a problem than a solution. Password systems are known to suffer from other disadvantages. Usually, passwords are specified by a user. Most users, being unsophisticated users of security systems, choose passwords which are relatively insecure. As such, many password systems are easily accessed through a simple trial and error process.

A security access system that provides substantially secure access and does not require a password or access code is a biometric identification system. A biometric identification system accepts unique biometric information from a user and identifies

the user by matching the information against information belonging to registered users of the system. One such biometric identification system is a fingerprint recognition system.

In a fingerprint input transducer or sensor, the finger under investigation is usually pressed against a flat surface, such as a side of a glass plate; the ridge and valley pattern of the finger tip is sensed by a sensing means such as an interrogating light beam.

Various optical devices are known which employ prisms upon which a finger whose print is to be identified is placed. The prism has a first surface upon which a finger is placed, a second surface disposed at an acute angle to the first surface through which the fingerprint is viewed and a third illumination surface through which light is directed into the prism. In some cases, the illumination surface is at an acute angle to the first surface, as seen for example, in US Patents 5,187,482 and 5,187,748. In other cases, the illumination surface is parallel to the first surface, as seen for example, in US Patents 5,109,427 and 5,233,404. Fingerprint identification devices of this nature are generally used to control the building-access or information-access of individuals to buildings, rooms, and devices such as computer terminals.

United States patent number 4,353,056 in the name of Tsikos issued October 5, 1982, discloses an alternative kind of fingerprint sensor that uses a capacitive sensing approach. The described sensor has a two dimensional, row and column, array of capacitors, each comprising a pair of spaced electrodes, carried in a sensing member and covered by an insulating film. The sensors rely upon deformation to the sensing member caused by a finger being placed thereon so as to vary locally the spacing between capacitor electrodes, according to the ridge/trough pattern of the fingerprint, and hence, the capacitance of the capacitors. In one arrangement, the capacitors of each column are connected in series with the columns of capacitors connected in parallel and a voltage is applied across the columns. In another arrangement, a voltage is applied to each individual capacitor in the array. Sensing in the respective two arrangements is accomplished by detecting the change of voltage distributi n in the series connected

capacitors or by measuring the voltage values of the individual capacitances resulting from local deformation. To achieve this, an individual connection is required from the detection circuit to each capacitor.

Before the advent of computers and imaging devices, research was conducted into fingerprint characterisation and identification. Today, much of the research focus in biometrics has been directed toward improving the input transducer and the quality of the biometric input data. A second important issue to be addressed is the identification process itself and more particularly, the registration process.

A common method of registering users for a biometric identification system is to capture biometric input information, characterise it, and store it as a template. The same user then provides biometric input information to the system for identification. This is repeated several times and if identification is successful, the user and their biometric template are registered. Further, the system requires an experienced operator to accept or reject instances of biometric information intended as templates.

A further method of registering users for a biometric identification system is to capture a plurality of instances of biometric input information from a same user and to characterise each instance. A composite biometric template is then constructed in dependence upon the plurality of instances provided. Such a system is complicated and it requires an experienced operator to accept or reject instances of biometric information intended for template construction.

Object of the Invention

It is an object of this invention to provide a means of selecting a biometric template or biometric information from which to derive a template.

It is an object of the invention to provide a method of training users to more effectively use biometric identification systems.

Summary of the Invention

In accordance with the invention there is provided a method of selecting a biometric template for use in registering biometric information from a source comprising the steps of:

providing a plurality of different instances of biometric information from the source to a processor;

using the processor, comparing the different instances of biometric information with other instances of biometric information, and determining a registration value corresponding to similarities or differences between each of the plurality of different instances and the other instances,

selecting as the biometric template an instance from the plurality of different instances for which the registration value is within predetermined limits.

The advantages of a system in accordance with this invention are numerous. For example, registration of authorized users requires little time and expense. The chance of deriving a biometric template from poor biometric information is greatly reduced.

Brief Description of the Drawings

An exemplary embodiment of the invention will now be described in conjunction with the attached drawings, in which:

Fig. 1a is a representation of a fingerprint image captured by an optical fingerprint imaging means;

Fig. 1b is a representation of another instance of a fingerprint image captured by an optical fingerprint imaging means imaging the same fingertip as that of Fig. 1a;

Fig. 1c is a representation of another instance of a fingerprint image captured by an optical fingerprint imaging means imaging the same fingertip as that of Fig. 1ε;

Fig. 2 is a flow diagram of a method of selecting a biometric template requiring 3 different biometric data sets in accordance with the invention;

Fig. 3 is a flow diagram of a further method of selecting a biometric template requiring n biometric data sets;

Fig. 4 is a flow diagram of a method of training users of a biometric input system according to the invention;

Fig. 5 is a flow diagram of a method reducing false acceptance (incorrect registration) of users of a biometric identification system according to the invention;

Fig. 6 is a flow diagram of a method of identifying the source of biometric input information in a system employing the method shown in the flow diagram of Fig. 5; and

Fig. 7 is a chart showing results from registrations using each of the fingerprint images of Figs. 1a, 1b, and 1c as templates and the others as biometric input information.

Detailed Description

The invention will be described with respect to finger print registration. The method of this invention is useful in other biometric template selection processes as well.

Referring to Figs. 1a, 1b, and 1c, a fingerprint is shown. A fingerprint is substantially unique and is identifiable by a series of criteria. These criteria include core size, core type, location of minutia, ridge spacing, ridge type, etc. Each feature can be located and stored for later registration of unknown prints. Unfortunately, accurately mapping out all features and determining registration based on partial prints and skewed prints is very time consuming; and, it is beneficial to minimize the time required to register a print. Therefore, not all features are analyzed to register each print.

A comparison of the fingerprint of Fig. 1a, Fig. 1b, and Fig. 1c will show them to have a same source; however, a comparison of the images directly is difficult as they are each different. Each time a person places a finger tip onto a fingerprint

scanner, a slightly different image is captured. From one instance to another a fingerprint may be shifted, skewed, cover different parts of the finger tip or be applied with different pressure. Since each captured image is substantially unique, it is likely that some images form better templates for registration than others. A method of selecting those fingerprints that form better templates is herein disclosed.

Referring to Fig. 2 a flow chart of a method according to the present invention is shown. Three instances of biometric information in the form of finger prints are captured. As shown in the flow diagram, each instance is captured individually. Preferably all instances are captured in such a way as to simulate normal use. For example, when using a fingerprint sensor for unlocking a door, a person steps up to the door and presses their finger tip against the sensor. The person then steps away from the door and approaches the door from a second different angle. In this way, the fingerprints imaged by the sensor will better reflect a variety of possible fingerprints from a same user during normal operation and each captured image is independent, excepting the relation to a known fingertip.

Preferably, an operator ensures that each image is a "good fingerprint" prior to storing the image for characterization. Operator skill is not required when using the method of this invention, but may result in an improved template.

Each fingerprint is then characterized. Fingerprint characterization is well known and can involve many aspects of fingerprint analysis. The analysis of fingerprints is discussed in the following references which are hereby incorporated by reference:

Xiao Qinghan and Bian Zhaoqi,: An approach to Fingerprint Identification By Using the Attributes of Feature Lines of Fingerprint," IEEE Pattern Recognition, pp 663, 1986

C.B. Shelman, " Fingerprint Classification - Theory and Application," Proc. 76 Carnahan Conference on Electronic Crime Countermeasures, 1976.

Feri Pernus, Stanko Kovacic, and Ludvik Gyergyek, "Minutaie Based Fingerprint Registration," IEEE Pattern Recognition, pp 1380, 1980.

J.A. Ratkovic, F.W. Blackwell, and H.H. Bailey, "Concepts for a Next Generation Automated Fingerprint System," Proc. 78 Carnahan Conference on Electronic Crime Countermeasures, 1978.

K. Millard, " An approach to the Automatic Retrieval of Latent Fingerprints," Proc. 75 Carnahan Conference on Electronic Crime Countermeasures, 1975.

Moayer and K.S. Fu, "A Syntactic Approach to Fingerprint Pattern Recognition," Memo Np. 73-18, Purdue University, School of Electrical Engineering, 1973.

Wegstein, *An Automated Fingerprint Identification System*, NBS special publication, U.S. Department of Commerce/National Bureau of Standards, ISSN 0083-1883; no. 500-89, 1982.

Moenssens, Andre A., Fingerprint Techniques, Chilton Book Co., 1971.

Wegstein and J.F. Rafferty, *The LX39 Latent Fingerprint Matcher*, NBS special publication, U.S. Department of Commerce/National Bureau of Standards; no. 500-36, 1978.

Using the method of the present invention, a same characterization method is employed in characterizing each fingerprint. This allows for comparisons between characterized images. Alternatively, a series of characterizations are performed on each fingerprint to determine a best fingerprint from which to select the template and a best characterization for the template. Use of multiple characterizations increases the overhead required to characterize a fingerprint during normal use. It will be apparent to those of skill in the art that when multiple characterizations are employed, only similarly characterized fingerprints are compared. The remainder of this description assumes the use of only one form of characterization.

Each characterized image is selected, one at a time, and all other characterized images are registered against the selected characterized image. The selected characterized image acts as a template and the remaining characterized images act as user input biometric information. This results in six registrations. For each characterized image (serving as a template) a score is achieved. The score is based on the correlation between the characterized image (as template) and the other characterized images. The six registrations produce six different scores,two for each characterized image, which

are compared. Alternatively, the scores for each characterized image, as template are added or averaged. The characterized image with the most desirable score(s) is selected to be the template. The score(s) is(are) then compared to a threshold value to determine suitability. When suitable, the image and the characterized image are stored and form the biometric information registration template. Alternatively, only the characterized image is stored. When the scores are not suitable, the characterized images are discarded and the method is followed again. Alternatively, only some characterized images are discarded and others are stored; the method is reapplied capturing only as many new images as are necessary in order to select a template.

In an alternative embodiment shown in Fig. 3, n instances of biometric information in the form of fingerprints are captured. Preferably, the captured images are independent as described above. Each image is characterized to produce a characterized image. At least some of the characterized images are selected. Against each of the characterized images selected, some other characterized images are registered. Should all characterized images be selected and compared against all other images, the number of resulting comparisons is (n) (n-1). For each registration, a resulting score is associated with the selected characterized image. The scores associated with each selected characterized image are compared and a characterized image with a most desirable set of scores is identified. The scores of the identified characterized image are verified against a threshold value to ensure that the identified characterized image is acceptable and the identified characterized image and the associated image are stored as a template. Alternatively, only the identified characterized image is stored as a template.

Alternatively, n instances of biometric information in the form of fingerprints are captured as shown in Fig. 3 and m further instances of biometric information in the form of fingerprints are provided. Preferably, the further images are selected to ensure a selected biometric template is unlikely to result in false registrations. The selection of the m instances is based on false authorizations that have occurred with some templates. Alternatively, the selection of the m instances is based on the

characterization of the n images. Alternatively, the selection of the m instances is based on a random selection. Against each of the characterized images from the n instances, some other characterized images are registered as are characterized images from the m instances. For each registration, a resulting score is associated with the selected characterized image. Scores indicative of similarities are desirable for registrations with characterized images from the n instances. Scores indicative of differences are desirable for characterized images from the m instances. The scores associated with each selected characterized image are compared and a characterized image with a most desirable set of scores is identified. Desirability of a set of scores is dependent on a predetermined level of security and on an application in which biometric identification is being used. The scores of the identified characterized image are verified against a threshold value to ensure that the identified characterized image is an acceptable template. Preferably, the template results in no authorization of instances from the m instances.

Preferably, the same characterized images are registered against each template. Further preferably, the scores are added or averaged.

Alternatively, the characterized image is modified prior to storing same. The modifications include removing features that failed to match similar features in at least some of the other characterized images. In this way, false features are reduced and improved registration results.

Most biometric identification systems work most effectively when users provide similar biometric input information each time they access a system. False rejections often result from inexperienced users of a biometric input device and more specifically from poor presentation of biometric information.

Referring to Fig. 4, a further use of a method according to this invention is automated training of users of biometric identification systems. A user provides a plurality of biometric input samples to a system. The system selects a sample as a template according to the present invention and reports on the resulting selected template and

the resulting score(s). A first sample is discarded and replaced by a new sample. This is repeated for several trials until the template and the score(s) are substantially similar between trials. Given that the score exceeds a predetermined threshold, it is likely that the user is providing biometric input information to the system that is useable for user identification.

In using biometric information in the form of fingerprint images for user identification, false registration is a great concern. Often, false registration is a function of the biometric information and not an "error" on the part of an identification system. Two different users may share many common features in their biometric information, and therefore, each may register as the other. In selecting templates, it would be advantageous to reduce false registration as much as possible. Referring to Fig. 5, a method of using a method according to the present invention for reducing false registration is presented. Templates are selected according to a known method of selecting same. A plurality of images are captured for each individual having a template. The images are each characterized and their characterizations are stored. Each image is registered against every template to identify potential false registrations. For large systems, such a task is very time consuming and would be best executed as a background task. When a possible false registration is identified, a further template is selected (from the images and characterized images) to distinguish between correct and false registration. The further template is stored with the original template in a hierarchical fashion. The task executes until all images have been registered against all templates.

Referring to Fig. 6, a flow diagram of a method of identifying a user in dependence upon biometric input information is shown for a system employing a method of reducing false registration as described with reference to Fig. 5. A user provides biometric information in the form of a fingerprint image. The image is characterized. The characterized image is compared against templates to locate user information. When a registration occurs (a template is sufficiently similar to the biometric information provided) the system verifies that false registration is unlikely.

When false registration is unlikely, registration is complete. When it is likely, the biometric information provided is compared to templates corresponding to each potential false registration associated with the registered template. When no further registration occurs, the registration process is complete.

When a further registration occurs, the registration process selects at least another template against which to verify the provided biometric information. This at least another template is stored associated with the templates against which registration has occurred. Selecting and storing the further template is described above with reference to Fig. 5. The further template improves the probability of distinguishing between each of the two potential false registrations identified.

Referring to Fig. 7, correlation results are shown for the finger prints of Fig. 1a, Fig. 1b, and Fig. 1c. The results indicate that registering a fingerprint on a second fingerprint is not commutative. As such, the number of registrations required to select a template can not be reduced by registering each pair only one time.

Alternatively, the method is employed with retinal scanned biometric information. Further alternatively, the method is employed with palm prints. Further alternatively, the method is employed with non image biometric data such as voice prints.

Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What we claim is:

1. A method of selecting a biometric template for use in registering biometric information from a source, comprising the steps of:
providing a plurality of different instances of biometric information from the source to a processor;
using the processor, selecting each instance of the plurality of different instances;
for each selected instance, using the processor comparing the selected instance with other instances of biometric information, and determining a registration value corresponding to similarities or differences between the selected instance and the other instances; and,
selecting as the biometric template an instance from the plurality of different instances for which the registration value is within predetermined limits.

2. A method of selecting a biometric template for use in registering biometric information of a source as defined in claim 1 further comprising the step of storing the selected biometric template.

3. A method of selecting a biometric template for use in registering biometric information of a source as defined in claim 1 wherein similarities or differences are determined in dependence upon a comparison between a different instance of biometric information and each other instance of biometric information and the registration value is determined in dependence upon similarities or differences.

4. A method of selecting a biometric template for use in registering biometric information of a source as defined in claim 3 wherein the registration value is an average of the similarities or differences.

5. A method of selecting a biometric template for use in registering biometric information of a source as defined in claim 1 further comprising the step of testing the registration value against a predetermined threshold value.

6. A method of selecting a biometric template for use in registering biometric information of a source as defined in claim 1 wherein similarities are indicative of a positive correlation and differences are indicative of a negative correlation.

7. A method of selecting a biometric template for use in registering biometric information of a source as defined in claim 1 further comprising the steps of determining a score for each instance of biometric information in dependence upon the registration values; and providing an output signal indicative of the scores.

8. A method of selecting a biometric template for use in registering biometric information from a biometric input device comprising the steps of:
providing a plurality of different instances of biometric information from the biometric input device to a processor;
selecting each instance of the plurality of different instances; and for each selected instance comparing that selected instance with other of the different instances of biometric information provided, and determining a registration value corresponding to similarities or differences between each selected instance; and,
selecting as the biometric template an instance from the plurality of different instances for which the registration value is within predetermined limits.

9. A method of selecting a biometric template for use in registering biometric information from a biometric input device as defined in claim 8 further comprising the steps of:
providing a second plurality of different instances of biometric information from the biometric input device to a processor; and
for each selected instance comparing that selected instance with instances of the second plurality of different instances of biometric information, and modifying the registration

value in dependence upon similarities or differences between each selected instance and instances of the second plurality of different instances of biometric information.

10. A method of selecting a biometric template for use in registering biometric information from a biometric input device comprising the steps of:
providing a plurality of different instances of biometric information from the biometric input device to a processor;
comparing each of the different instances with other of the plurality of different instances of biometric information provided, and for each comparison, determining a registration value corresponding to similarities or differences between each different instance and the plurality of other different instances; and,
selecting as the biometric template an instance from the plurality of different instances for which the registration value is within predetermined limits.

a0000404.i

Fig. 1a

b0000404.i

Fig. 1b

c0000404.i

Fig. 1c

Fig. 2

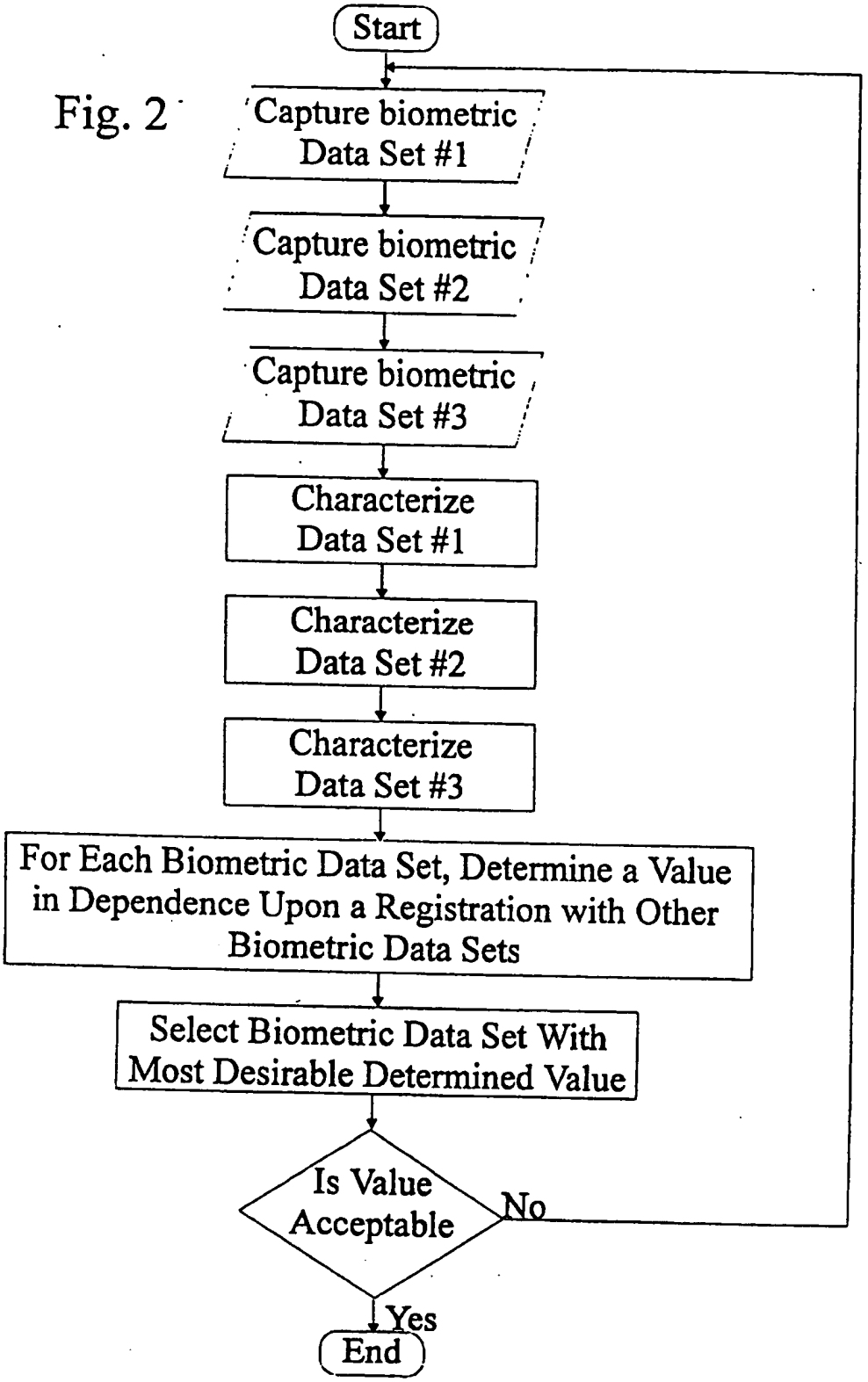

Start
Capture biometric Data Set #1
Capture biometric Data Set #2
Capture biometric Data Set #3
Characterize Data Set #1
Characterize Data Set #2
Characterize Data Set #3
For Each Biometric Data Set, Determine a Value in Dependence Upon a Registration with Other Biometric Data Sets
Select Biometric Data Set With Most Desirable Determined Value
Is Value Acceptable
No
Yes
End

Fig. 3

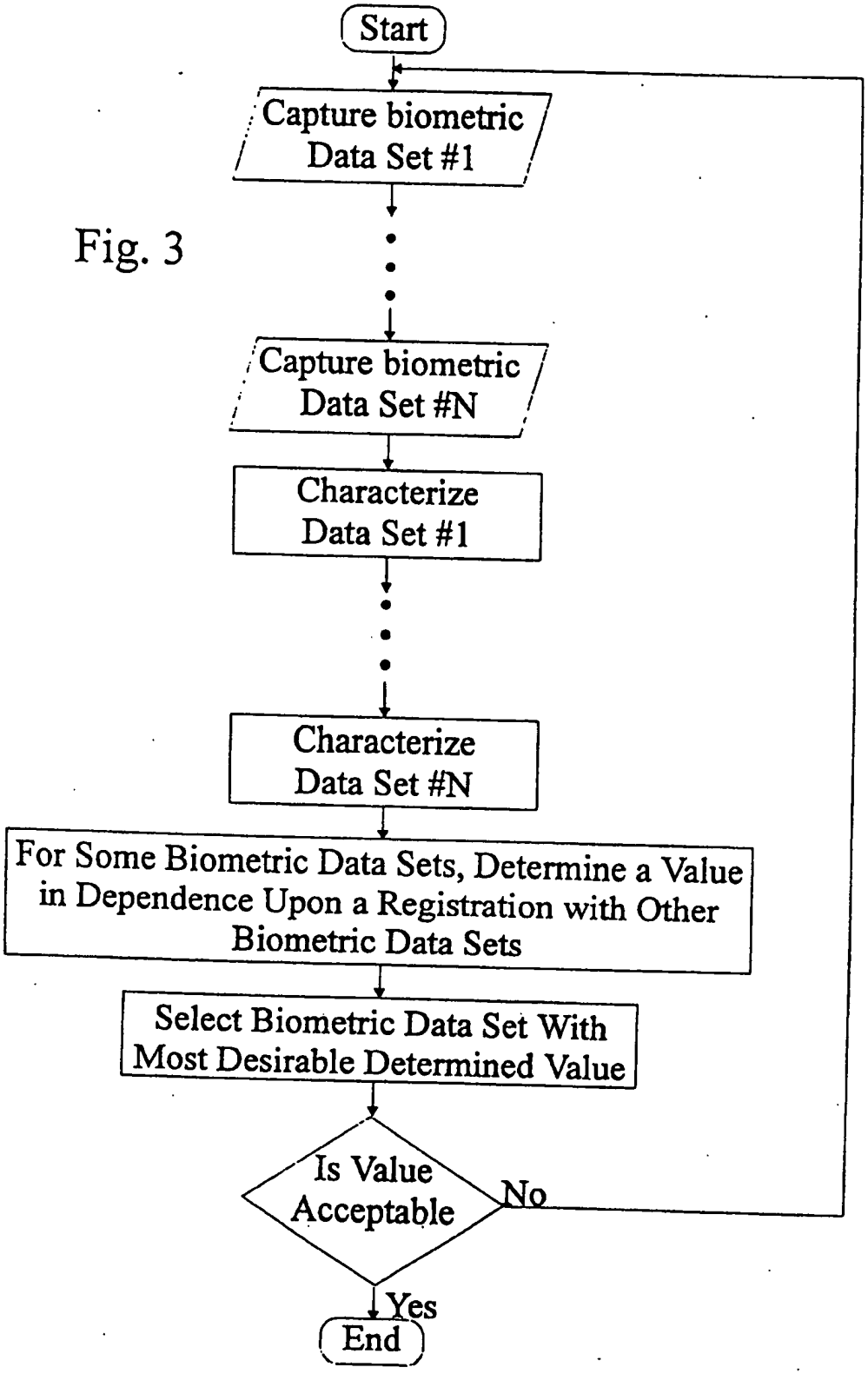

Start
Capture biometric Data Set #1
Capture biometric Data Set #N
Characterize Data Set #1
Characterize Data Set #N
For Some Biometric Data Sets, Determine a Value in Dependence Upon a Registration with Other Biometric Data Sets
Select Biometric Data Set With Most Desirable Determined Value
Is Value Acceptable
No
Yes
End

Fig. 4

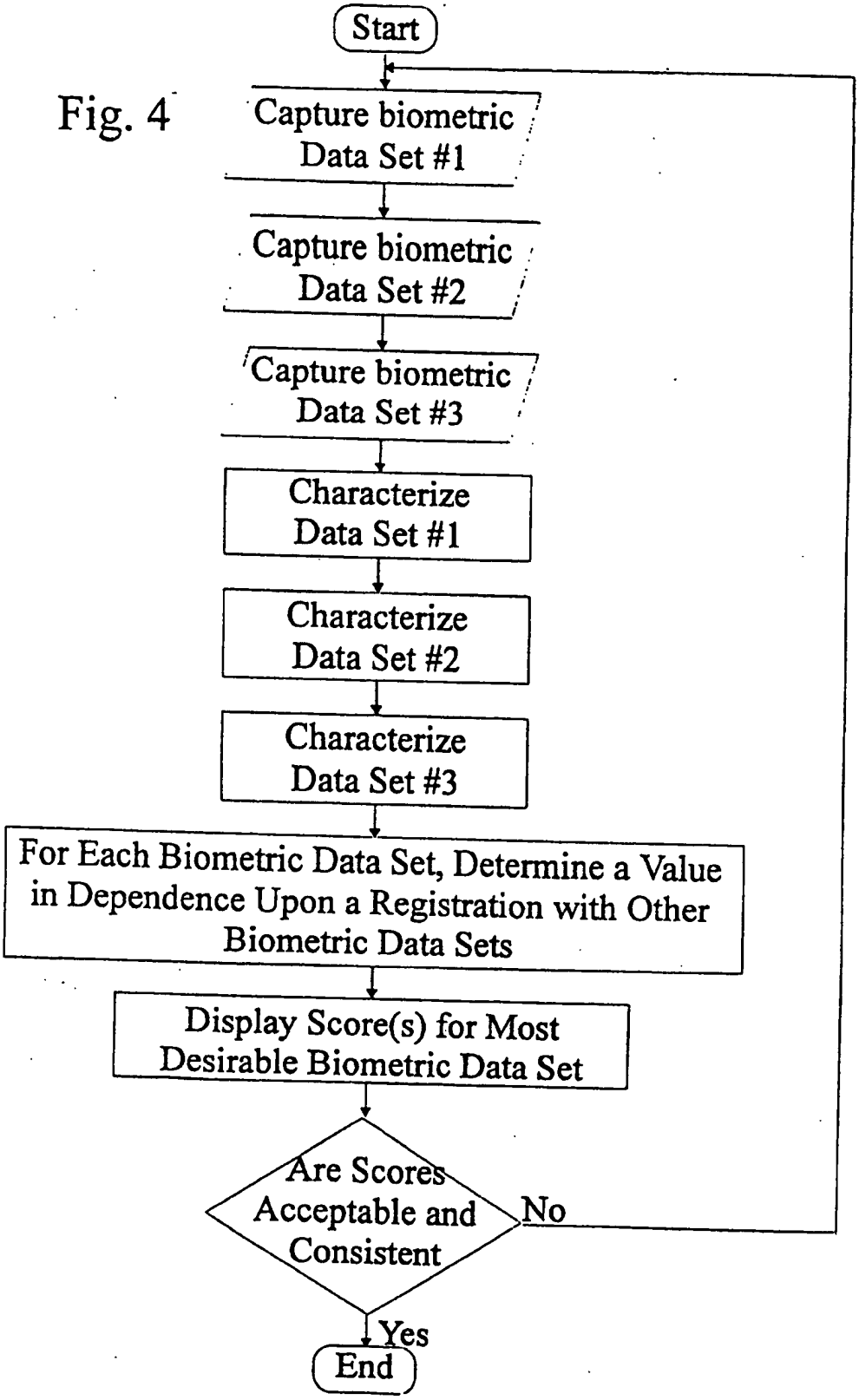

Start
Capture biometric Data Set #1
Capture biometric Data Set #2
Capture biometric Data Set #3
Characterize Data Set #1
Characterize Data Set #2
Characterize Data Set #3
For Each Biometric Data Set, Determine a Value in Dependence Upon a Registration with Other Biometric Data Sets
Display Score(s) for Most Desirable Biometric Data Set
Are Scores Acceptable and Consistent
No
Yes
End

Fig. 5

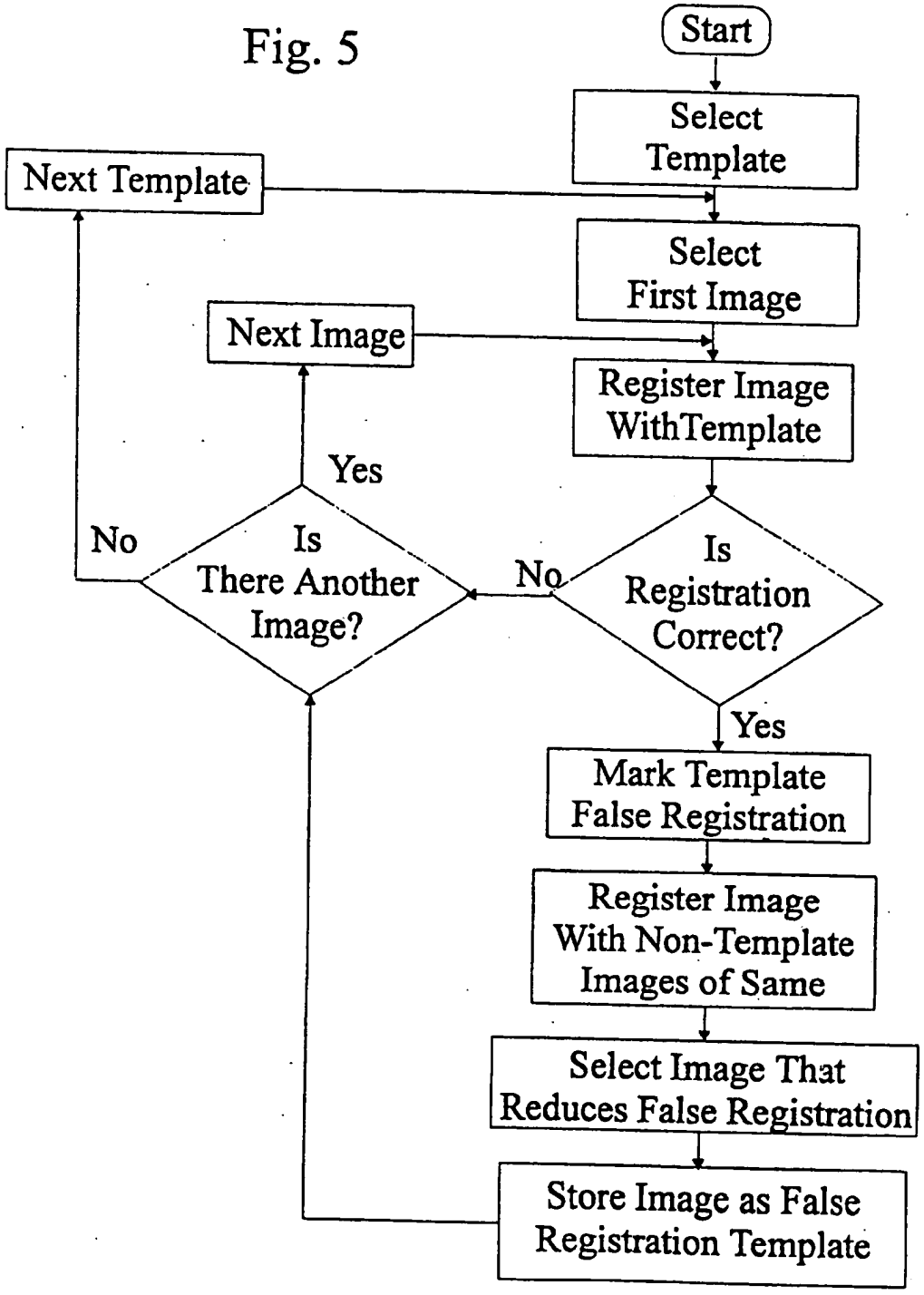

Start
Select Template
Next Template
Select First Image
Next Image
Register Image WithTemplate
Yes
No
Is There Another Image?
No
Is Registration Correct?
Yes
Mark Template False Registration
Register Image With Non-Template Images of Same
Select Image That Reduces False Registration
Store Image as False Registration Template

Fig. 6

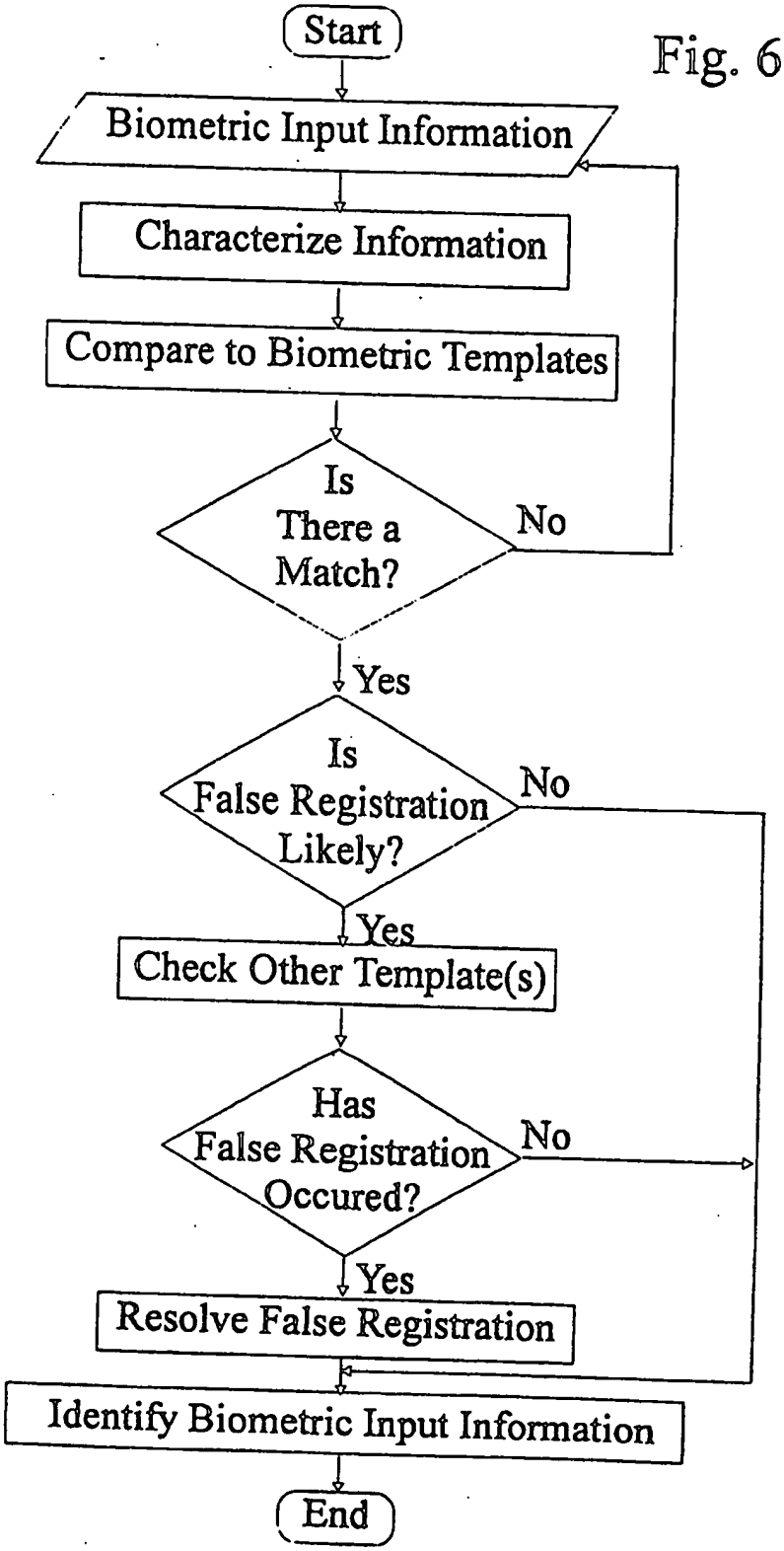

Start
Biometric Input Information
Characterize Information
Compare to Biometric Templates
Is There a Match?
No
Yes
Is False Registration Likely?
No
Yes
Check Other Template(s)
Has False Registration Occured?
No
Yes
Resolve False Registration
Identify Biometric Input Information
End

Table of comparison scores for
3 instances of same fingerprint

a0000404.i vs b0000404.i: 54.01
a0000404.i vs c0000404.i: 64.22
b0000404.i vs a0000404.i: 40.09
b0000404.i vs c0000404.i: 86.20
c0000404.i vs a0000404.i: 32.87
c0000404.i vs b0000404.i: 79.20

Fig. 7

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/CA 97/00924

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K9/00 G06K9/62

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LIU C N: "REFERENCE DESIGN PROCEDURE FOR SIGNATURE VERIFICATION" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 21, no. 1, June 1978, page 426/427 XP002050797 see the whole document	1-3,5, 7-10
A	GB 2 271 657 A (BRITISH TECH GROUP) 20 April 1994 see page 9, line 12 - page 10, line 9; figures 2,5	1-10
A	EP 0 426 423 A (KOKUSAN KINZOKU KOGYO KK) 8 May 1991 see figures 1,3	1-10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 March 1998	11/03/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Granger, B

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/CA 97/00924

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 802 231 A (DAVIS ELLIOT) 31 January 1989 see abstract; figure 1	6

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...ormation on patent family members

Inter nal Application No
PCT/CA 97/00924

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2271657 A	20-04-94	EP 0664913 A	02-08-95
		WO 9409448 A	28-04-94
		JP 8502376 T	12-03-96
EP 0426423 A	08-05-91	JP 3142685 A	18-06-91
		DE 69026466 D	15-05-96
		DE 69026466 T	02-10-96
		KR 9409714 B	17-10-94
		US 5210797 A	11-05-93
US 4802231 A	31-01-89	EP 0389541 A	03-10-90
		JP 3501657 T	11-04-91
		WO 8905015 A	01-06-89